CLAIMS

1. (currently amended) A method of securing data in a computer network against a plurality of computer events with an electronic attack monitor generating a corresponding plurality of attack warnings, said data, sought to be secured, having one or more security sensitive words, characters, icons or data objects, said computer network having, interconnected together, a plurality of computers for a plurality of users having a corresponding a plurality of security levels each with a respective security clearance, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, respective memories designated as a remainder store and respective extract stores for said plurality of security levels in one or more computers of said plurality of computers, comprising:

filtering data input from said data input computer dependent upon respective ones of said plurality of attack warnings and extracting said security sensitive words, characters, icons or data objects from said data to obtain extracted data and remainder data, the degree of extraction dependent upon respective ones of said plurality of attack warnings;

storing said extracted data and said remainder data in said respective extract stores and said remainder store based upon respective ones of said plurality of attack warnings; and,

permitting reconstruction of some or all of said data via said extracted data from ~~respected~~ respective extract stores and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

2. (original) A method as claimed in claim 1 wherein the method including encrypting said extracted data with corresponding degrees of encryption dependent upon respective ones of said plurality of attack warnings and including decrypting, during the reconstruction, of some or all of

said extracted data only in the presence of said respective security level of said plurality of security levels.

3. (original) A method as claimed in claim 1 wherein said plurality of computers define a plurality of extract stores, and the method includes extracting subsets of extracted data and storing said subsets of extracted data in said plurality of extract stores dependent upon respective ones of said plurality of attack warnings.

4. (original) A method as claimed in claim 1 including defining a plurality of filters, corresponding to respective ones of said plurality of attack warnings, prior to said filtering step.

5. (original) A method as claimed in claim 2 wherein the step of permitting reconstruction includes decrypting said extracted data.

6. (original) A method as claimed in claim 1 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the method including sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

7. (original) A method as claimed in claim 1 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays dependent upon respective ones of said plurality of attack warnings.

8. (original) A method as claimed in claim 1 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein the reconstruction step of the method includes interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments dependent upon respective ones of said plurality of attack warnings.

9. (original) A method as claimed in claim 1 including deleting said data input from said data input computer after the step of storing.

10. (original) A method as claimed in claim 1 including mapping said storing of extracted data.

11. (original) A method as claimed in claim 2 including encrypting said remainder data prior to storing dependent upon respective ones of said plurality of attack warnings.

12. (original) A method as claimed in claim 11 wherein the step of permitting reconstruction includes decrypting said remainder data.

13. (original) A method as claimed in claim 12 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said storing utilizes the URL for one or both of said extract store and said remainder store.

14. (original) A method as claimed in claim 12 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the

method including sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

15. (original) A method as claimed in claim 14 including the step of encrypting and decrypting said remainder data and extracted data during sending and downloading.

16. (original) A method as claimed in claim 15 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays dependent upon respective ones of said plurality of attack warnings.

17. (original) A method as claimed in claim 15 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein the reconstruction step of the method includes interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments dependent upon respective ones of said plurality of attack warnings.

18. (original) A method as claimed in claim 15 including deleting said data input from said data input computer after the step of storing.

19. (original) A method as claimed in claim 18 including mapping said storing of said extracted data.

20. (original) A method as claimed in claim 1 wherein one of the steps of filtering, storing and permitting reconstruction utilize one of an inference engine, neural network and artificial intelligence process to filter, store and permit reconstruction.

21. (original) A method as claimed in claim 1 wherein said security sensitive data objects are one or more portions of an audio file and the step of reconstruction utilizes extracted data representative of said one or more portions of said audio file.

22. (original) A method as claimed in claim 1 wherein said plurality of computer events includes hacking attacks, power loss, environmental conditions adverse to said computer network, said electronic attack monitor including sensory systems responsive to said plurality of computer events to generate said plurality of attack warnings, and the filtering and storing responsive to said plurality of computer events which include said hacking attacks, power loss, environmental conditions adverse to said computer network.

23. (previously amended) A computer readable medium containing programming instructions for securing data in a computer network against a plurality of computer events with an electronic attack monitor generating a corresponding plurality of attack warnings, said data, sought to be secured, having one or more security sensitive words, characters, icons or data objects, said computer network having, interconnected together, a plurality of computers for a plurality of users having a corresponding a plurality of security levels each with a respective security clearance, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, respective memories designated as a remainder store and respective extract stores for said plurality of security levels in one or more computers of said plurality of computers, the programming instructions comprising:

filtering data input from said data input computer dependent upon respective ones of said plurality of attack warnings and extracting said security sensitive words, characters, icons or data

objects from said data to obtain extracted data and remainder data, the degree of extraction dependent upon respective ones of said plurality of attack warnings;

storing said extracted data and said remainder data in said respective extract stores and said remainder store based upon respective ones of said plurality of attack warnings; and,

permitting reconstruction of some or all of said data via said extracted data from said respective extract stores and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

24. (original) A medium with programming instructions as claimed in claim 23 including encrypting said extracted data with corresponding degrees of encryption dependent upon respective ones of said plurality of attack warnings and including decrypting, during the reconstruction, of some or all of said extracted data only in the presence of said respective security level of said plurality of security levels.

25. (original) A medium with programming instructions as claimed in claim 23 wherein said plurality of computers define a plurality of extract stores, and the instructions include extracting subsets of extracted data and storing said subsets of extracted data in said plurality of extract stores dependent upon respective ones of said plurality of attack warnings.

26. (original) A medium with programming instructions as claimed in claim 23 including defining a plurality of filters, corresponding to respective ones of said plurality of attack warnings, prior to said filtering step.

27. (original) A medium with programming instructions as claimed in claim 26 wherein the step of permitting reconstruction includes decrypting said extracted data.

28. (original) A medium with programming instructions as claimed in claim 23 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the instructions including sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

26. (original) A medium with programming instructions as claimed in claim 23 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the reconstruction instruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays dependent upon respective ones of said plurality of attack warnings.

30. (original) A medium with programming instructions as claimed in claim 23 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein the reconstruction instruction includes interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments dependent upon respective ones of said plurality of attack warnings.

31. (original) A medium with programming instructions as claimed in claim 23 including deleting said data input from said data input computer after storing.

32. (original) A medium with programming instructions as claimed in claim 23including mapping said storing of extracted data.

33. (original) A medium with programming instructions as claimed in claim 24 including encrypting said remainder data prior to storing dependent upon respective ones of said plurality of attack warnings.

34. (original) A medium with programming instructions as claimed in claim 33 wherein permitting reconstruction includes decrypting said remainder data.

35. (original) A medium with programming instructions as claimed in claim 34 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said storing utilizes the URL for one or both of said extract store and said remainder store.

36. (original) A medium with programming instructions as claimed in claim 34 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the instructions include sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

37. (original) A medium with programming instructions as claimed in claim 36 including encrypting and decrypting said remainder data and extracted data during sending and downloading.

38. (original) A medium with programming instructions as claimed in claim 37 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the reconstruction instruction including displaying said extracted data on one of said at least two displays and displaying said

remainder data on another of said at least two displays dependent upon respective ones of said plurality of attack warnings.

39. (original) A medium with programming instructions as claimed in claim 37 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein the reconstruction includes interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments dependent upon respective ones of said plurality of attack warnings.

40. (original) A medium with programming instructions as claimed in claim 37 including deleting said data input from said data input computer after the step of storing.

41. (original) A medium with programming instructions as claimed in claim 40 including mapping said storing of said extracted data.

42. (original) A medium with programming instructions as claimed claim 23 wherein the programming instructions for one of the filtering, storing and permitting reconstruction utilize one of an inference engine, neural network and artificial intelligence process to filter, store and permit reconstruction.

43. (original) A medium with programming instructions as claimed claim 42 wherein the programming instructions for the filtering increases extraction with said inference engine based upon increasingly higher attack levels.

44. (original) A medium with programming instructions as claimed claim 23 wherein said security sensitive data objects are one or more portions of an audio file and the programming instructions for reconstruction utilizes extracted data representative of said one or more portions of said audio file.

45. (original) A medium with programming instructions as claimed claim 23 wherein said plurality of computer events includes hacking attacks, power loss, environmental conditions adverse to said computer network, said electronic attack monitor including sensory systems responsive to said plurality of computer events to generate said plurality of attack warnings, and the programming instructions for filtering and storing is responsive to said plurality of computer events which include said hacking attacks, power loss, environmental conditions adverse to said computer network.

46. (currently amended) An information processing system for securing data in a computer network against a plurality of computer ~~hacking~~ events with ~~a hacking~~ an attack monitor generating a corresponding plurality of ~~hack~~ attack warnings, said data, sought to be secured, having one or more security sensitive words, characters, icons or data objects, said computer network having, interconnected together, a plurality of computers for a plurality of users having a corresponding a plurality of security levels each with a respective security clearance, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, respective memories designated as a remainder store and respective extract stores for said plurality of security levels in one or more computers of said plurality of computers, comprising:

means for filtering data input from said data input computer dependent upon respective ones of said plurality of attack warnings and extracting said security sensitive words, characters, icons or data objects from said data to obtain extracted data and remainder data, the degree of extraction dependent upon respective ones of said plurality of attack warnings;

means for storing said extracted data and said remainder data in said respective extract stores and said remainder store based upon respective ones of said plurality of attack warnings; and,

means for permitting reconstruction of some or all of said data via said extracted data in said respective extract stores and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

47. (original) An information processing system as claimed in claim 46 including means for encrypting said extracted data with corresponding degrees of encryption dependent upon respective ones of said plurality of attack warnings and including means for decrypting, during the reconstruction, of some or all of said extracted data only in the presence of said respective security level of said plurality of security levels.

48. (original) An information processing system as claimed in claim 46 wherein said plurality of computers define a plurality of extract stores, and the system includes means for extracting subsets of extracted data and storing said subsets of extracted data in said plurality of extract stores dependent upon respective ones of said plurality of attack warnings.

49. (original) An information processing system as claimed in claim 46 including means for defining a plurality of filters, corresponding to respective ones of said plurality of attack warnings, prior to said filtering.

50. (original) An information processing system as claimed in claim 49 wherein the means for reconstruction includes means for decrypting said extracted data.

51. (original) An information processing system as claimed in claim 46 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the system including means for sending said extracted data from said data input

computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

52. (original) An information processing system as claimed in claim 46 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the means for reconstruction including means for displaying said extracted data on one of said at least two displays and means for displaying said remainder data on another of said at least two displays dependent upon respective ones of said plurality of attack warnings.

53. (original) An information processing system as claimed in claim 46 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality of frame memory segments, and wherein the means for reconstruction includes means for interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments dependent upon respective ones of said plurality of attack warnings.

54. (original) An information processing system as claimed in claim 46 including means for deleting said data input from said data input computer after storing.

55. (original) An information processing system as claimed in claim 46 including means for mapping said storing of extracted data.

56. (original) An information processing system as claimed in claim 47 including means for encrypting said remainder data prior to storing dependent upon respective ones of said plurality of attack warnings.

57. (original) An information processing system as claimed in claim 56 wherein the means for permitting reconstruction includes means for decrypting said remainder data.

58. (original) An information processing system as claimed in claim 57 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said means for storing utilizes the URL for one or both of said extract store and said remainder store.

59. (original) An information processing system as claimed in claim 57 wherein said plurality of computers are configured in a client-server network within which respective computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in said client-server network and one of said plurality of computers is designated as a server computer, the system including means for sending said extracted data from said data input computer to the computer with said extract store utilizing the respective URL as controlled by said server computer.

60. (original) An information processing system as claimed in claim 59 including means for encrypting and decrypting said remainder data and extracted data during sending and downloading.

61. (original) An information processing system as claimed in claim 60 wherein one computer of said plurality of computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the means for reconstruction including means for displaying said extracted data on one of said at least two displays and means for displaying said remainder data on another of said at least two displays dependent upon respective ones of said plurality of attack warnings.

62. (original) An information processing system as claimed in claim 60 wherein one computer of said plurality of computers includes a display fed from video memory having a plurality

of frame memory segments, and wherein the means for reconstruction includes means for interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments dependent upon respective ones of said plurality of attack warnings.

63. (original) An information processing system as claimed in claim 60 including means for deleting said data input from said data input computer after storing.

64. (original) An information processing system as claimed in claim 63 including means for mapping said storing of said extracted data.

65. (original) An information processing system as claimed in claim 46 wherein one of the means for filtering, means for storing and means for permitting reconstruction utilize one of an inference engine, neural network and artificial intelligence process to filter, store and permit reconstruction.

66. (original) An information processing system as claimed in claim 46 wherein said security sensitive data objects are one or more portions of an audio file and said means for reconstruction utilizes extracted data representative of said one or more portions of said audio file.

67. (currently amended) An information processing system as claimed in claim 46 wherein said plurality of computer events includes hacking attacks, power loss, environmental conditions adverse to said computer network, said ~~electronic~~ attack monitor including sensory systems responsive to said plurality of computer events to generate said plurality of attack warnings, and said means for filtering and for storing being responsive to said plurality of computer events which include said hacking attacks, power loss, environmental conditions adverse to said computer network.